Network/Service/Application Operations
It’s about the Data

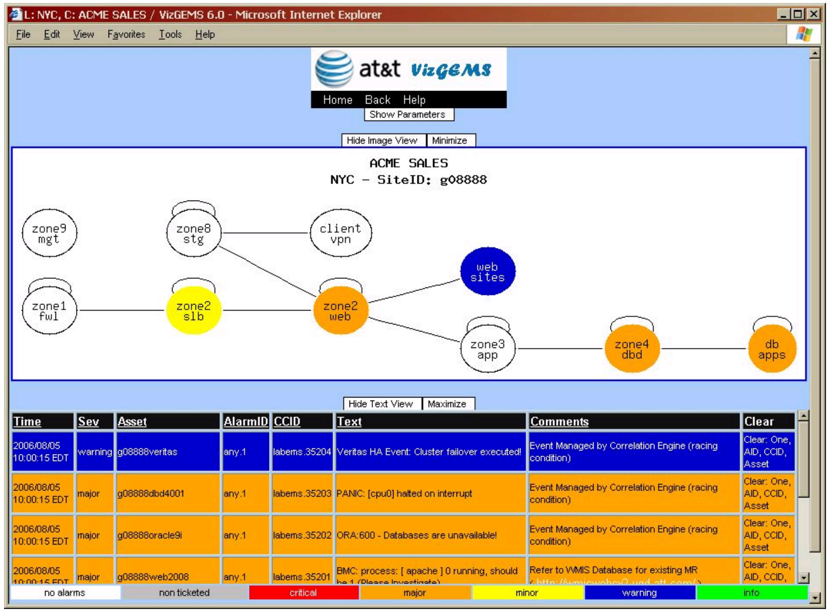
Dr. David Belanger

AT&T Labs Chief Scientist, and
V. P. Information & Software Systems Research

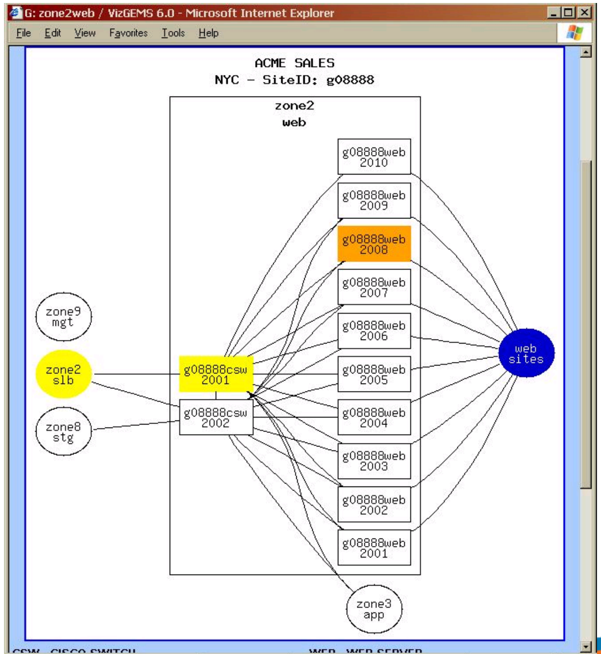
© 2007 AT&T Intellectual Property. All rights reserved. AT&T
and the AT&T logo are trademarks of AT&T Intellectual Property.

Operations – Give me all your data

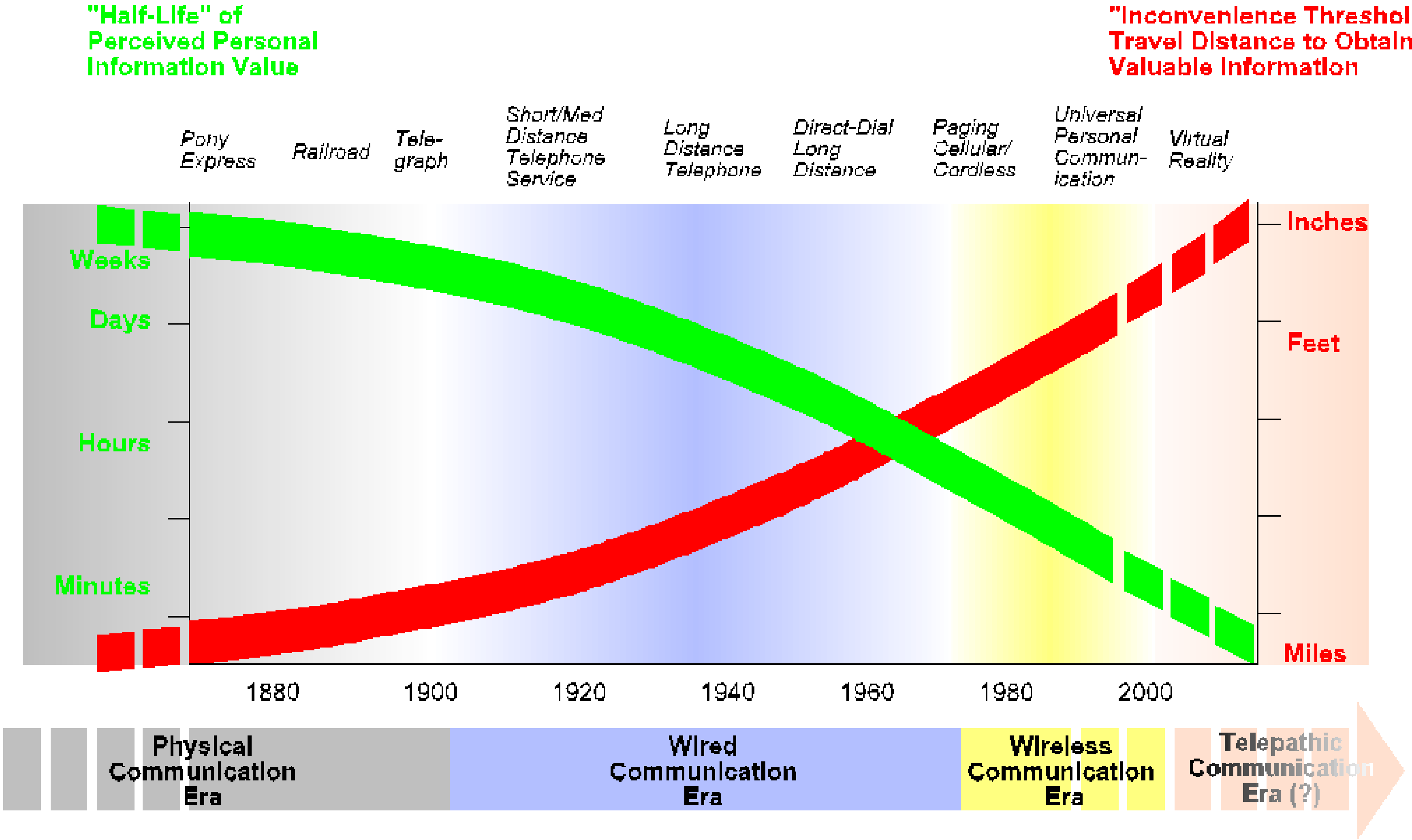
Operations is increasingly about End-to-End control across multiple networks/services; across multiple layers in network, computing, and software stacks; and, across a variety of time-frames. It is, therefore, a problem of integration of huge amounts of very heterogeneous data in real time.



Time	Sev	Asset	AlarmID	CCID	Text	Comments	Clear
2006/08/05 10:00:15 EDT	warning	g08888veritas	any.1	labems.35204	Veritas HA Event: Cluster failover executed!	Event Managed by Correlation Engine (racing condition)	Clear: One, AID, CCID, Asset
2006/08/05 10:00:15 EDT	major	g08888dbd4001	any.1	labems.35203	PANIC: [cpu0] halted on interrupt	Event Managed by Correlation Engine (racing condition)	Clear: One, AID, CCID, Asset
2006/08/05 10:00:15 EDT	major	g08888oracle9i	any.1	labems.35202	ORA:600 - Databases are unavailable!	Event Managed by Correlation Engine (racing condition)	Clear: One, AID, CCID, Asset
2006/08/05	major	g08888web2008	any.1	labems.35201	BMC: process: [apache] 0 running, should	Refer to VMIS Database for existing MR	Clear: One, AID, CCID,



"Half Life" and "Inconvenience Threshold"



Each communication technology advance has shortened the useful life of information and increased the need to obtain new information more rapidly regardless of the situation or location…

4/27/2010

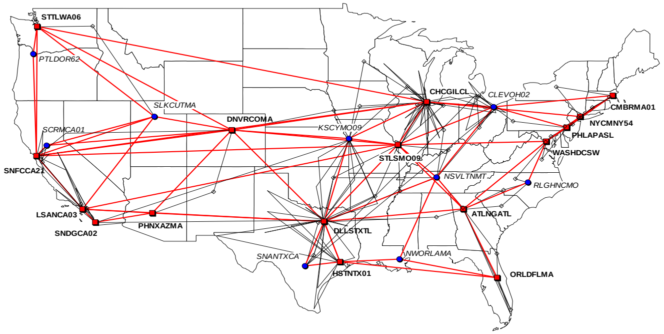
Operations Today

Operations

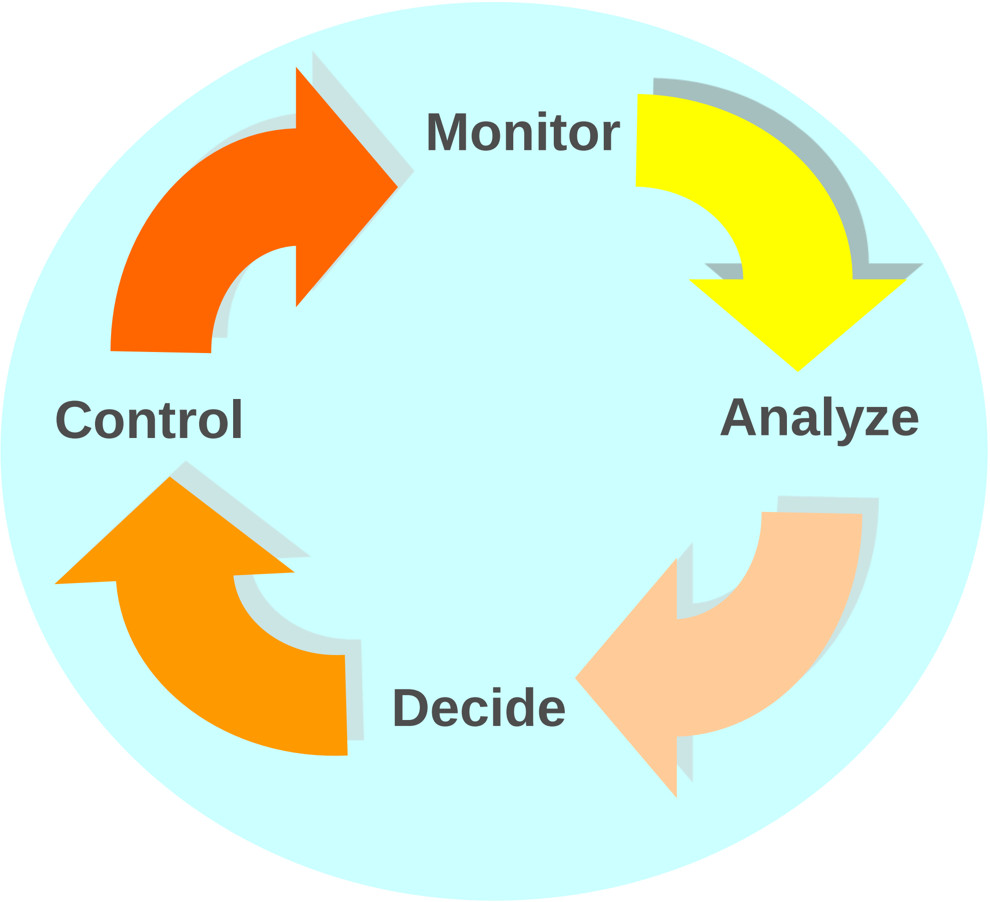
Services

Applications

Network



Operations Cycle

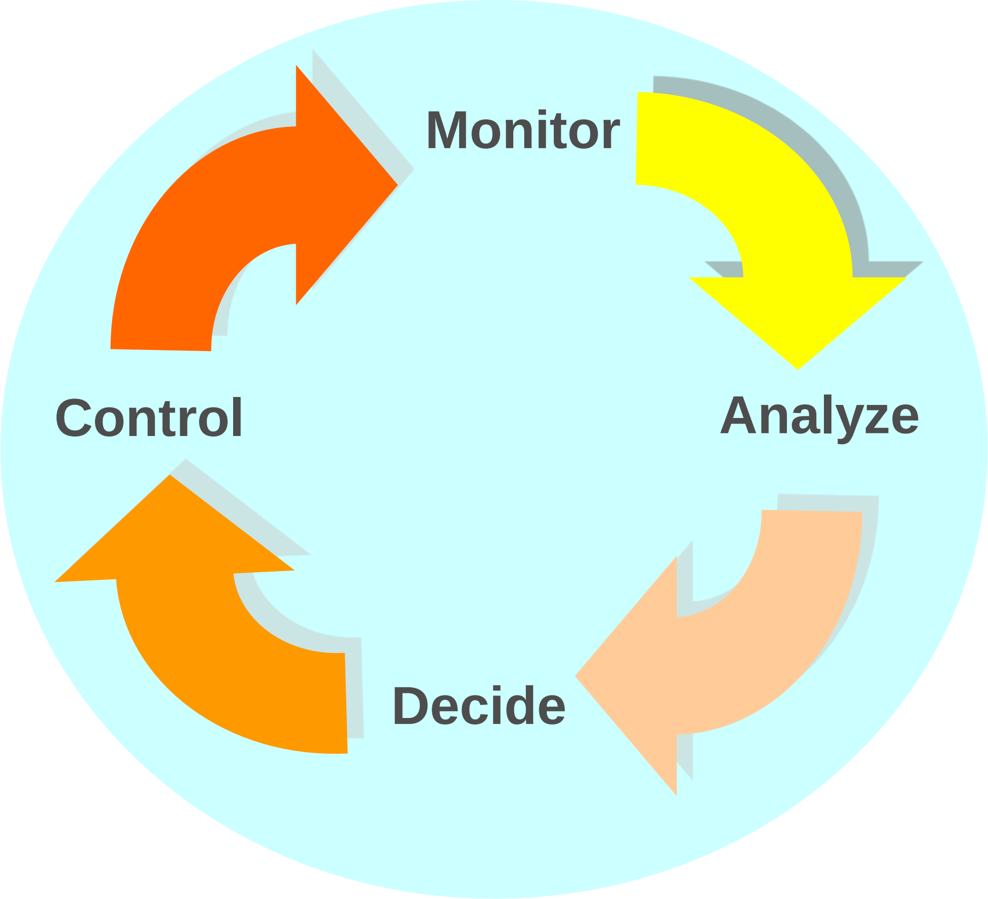


Each phase can be complex in large networked systems

- Monitoring involves data across multiple hosts and multiple sources.
- Analyzing may involve heuristics or evaluation over time.
- Decision may involve evaluating tradeoffs or distributed algorithms.
- Control may involve distributed coordination across multiple hosts.

All done in a running system and an environment that continues to change.

Operations Cycle

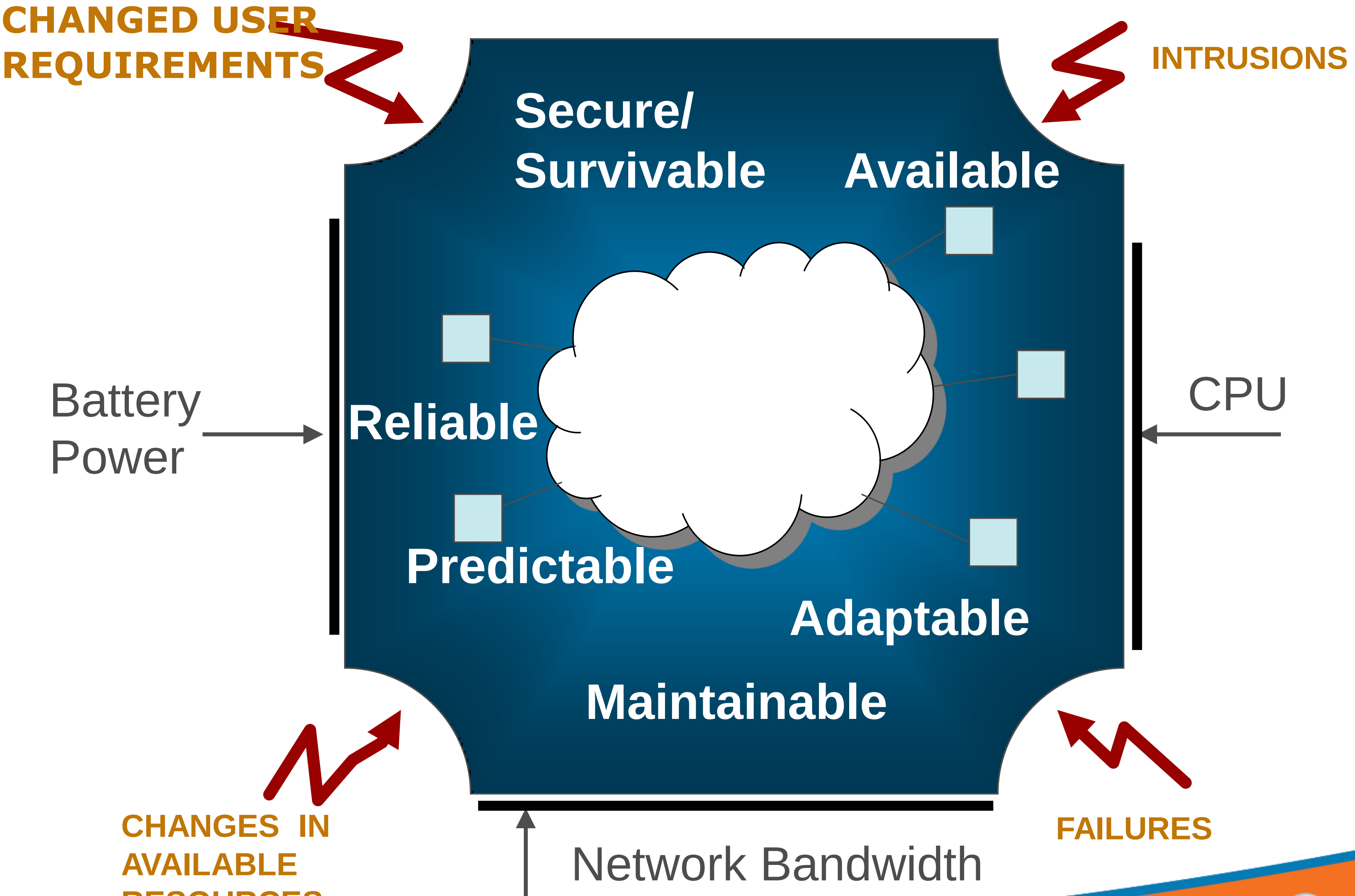


This often involves huge amounts, and many types, of data:

- Examples may include:
  - Circuit Switched Networks – SS7, CDR, …
  - IP Networks - Netflow, SNMP, …
  - Mobile Networks – UE, Physical & Location, RNC/MSC, …
  - Systems – Logs, utilization, virtualization, …
  - Sensors – SmartGrid, TeleHealth, RFID, …

Data flows are very widely distributed, and often measure in the Giga/Tera/Peta Bytes per day.

Systems Environment



CHANGED USER REQUIREMENTS

INTRUSIONS

Secure/ Survivable

Available

Reliable

Predictable

Adaptable

Maintainable

Battery Power

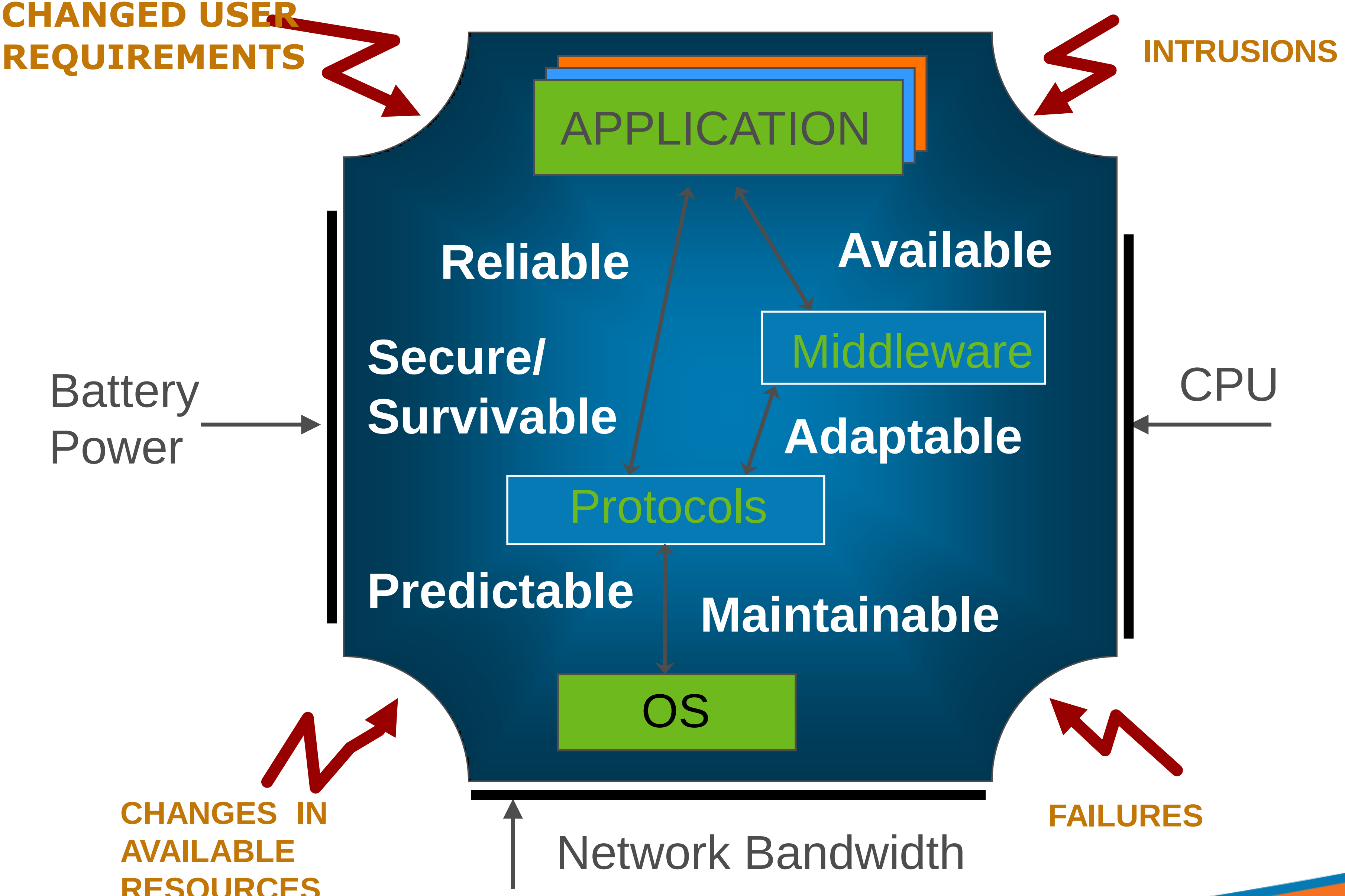
CPU

Network Bandwidth

CHANGES IN AVAILABLE RESOURCES

FAILURES

Control in Systems Environment



CHANGED USER REQUIREMENTS

INTRUSIONS

APPLICATION

Reliable

Available

Secure/ Survivable

Middleware

Battery Power

CPU

Adaptable

Protocols

Predictable

Maintainable

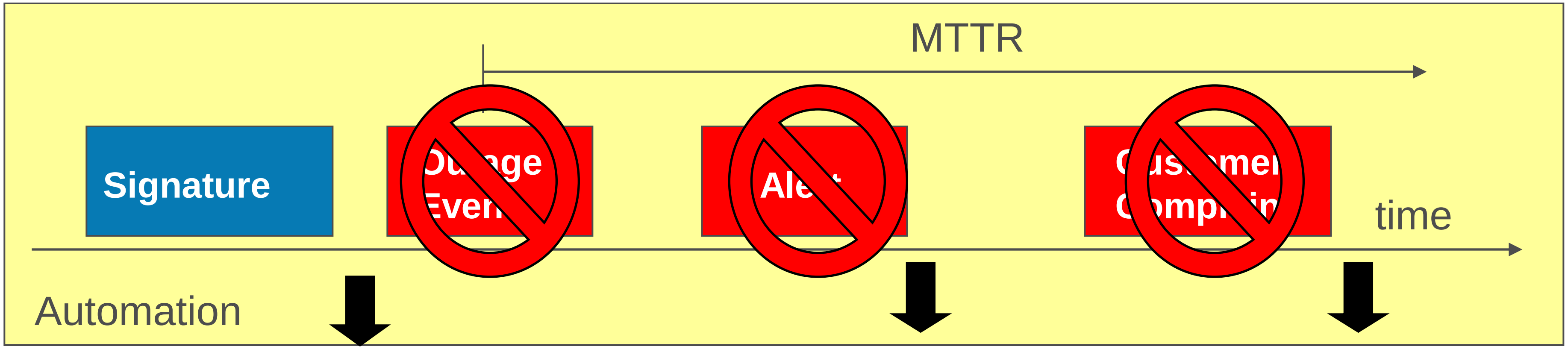
OS

CHANGES IN AVAILABLE RESOURCES

FAILURES

Network Bandwidth

Network Based Computing:
Goal - Adaptive Maintenance



Predictive maintenance

- Eliminates MOOs and outages
- Further reduces costs, including overtime pay
- Tradeoff of maintenance and outage costs
- Delighted customers

Proactive maintenance

- Reduces MOOs and MTTR
- Reduces operational costs
- Customer care costs reduced
- Automated customer status
- Happier customers

Reactive maintenance

- Highest MOOs
- SLA risk
- High care costs
- Disappointed customers

Adaptive maintenance

§ Reduces false positives and unnecessary costs

Scale – Still the Heart of the Challenge

Scale includes volume, volatility, complexity, reliability, and security.

3,600,000,000,000,000,000,000

Report on American Consumers

Roger E. Bohn & James E. Short

Global Information Industry Center, UCSD

Industry–University Collaborations

AT&T, Cisco Systems, IBM, Intel Corporations, LSI, Oracle, Seagate Technology

How Much Information? 2009

- **The goal of HMI? Project is to create a census of the world's data and information**
- **First Report: Information at the US Consumer Level**
- **How Much Information was Consumed by Individuals in the U.S. in 2008?**

3.6 Zettabytes (ZB = 10^21 bytes)

- ***How much is 3.6 Zettabytes?*** **If we printed 3.6 zettabytes of text in books, and stacked them as tightly as possible across the United States including Alaska, the pile would be 7 feet high**

How Much Information? 2009

- **Measures of information include all data delivered to people, whether for personal consumption, for communication or for any other reason: Cable TV, Broadcast TV, Radio, Telephone Line, Internet, Wireless, etc.**

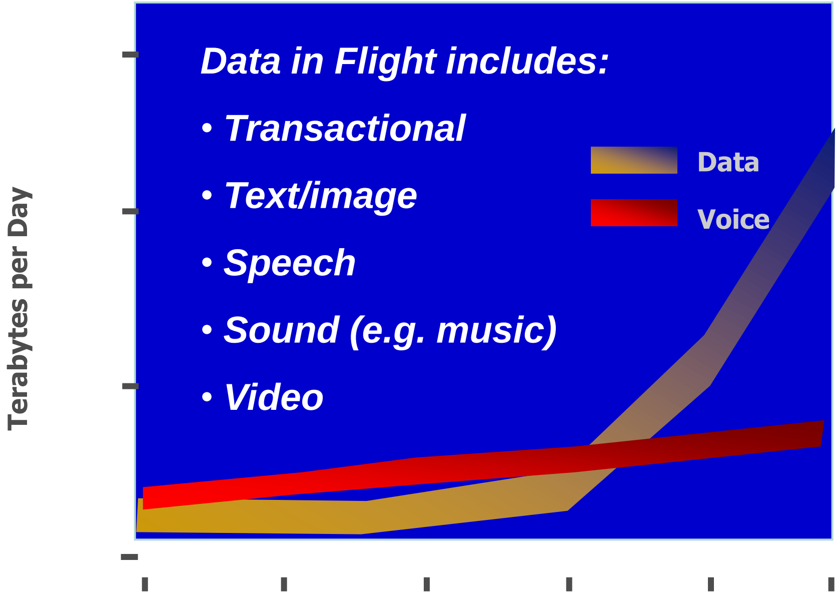
Network Data

- ***The AT&T Network***
  - ***Currently carries 18.7 Petabytes of data traffic on an average business day (PB = 10^15 bytes)***
  - **Nearly 5 Billion calls per day**

Information in Flight

Information in Flight

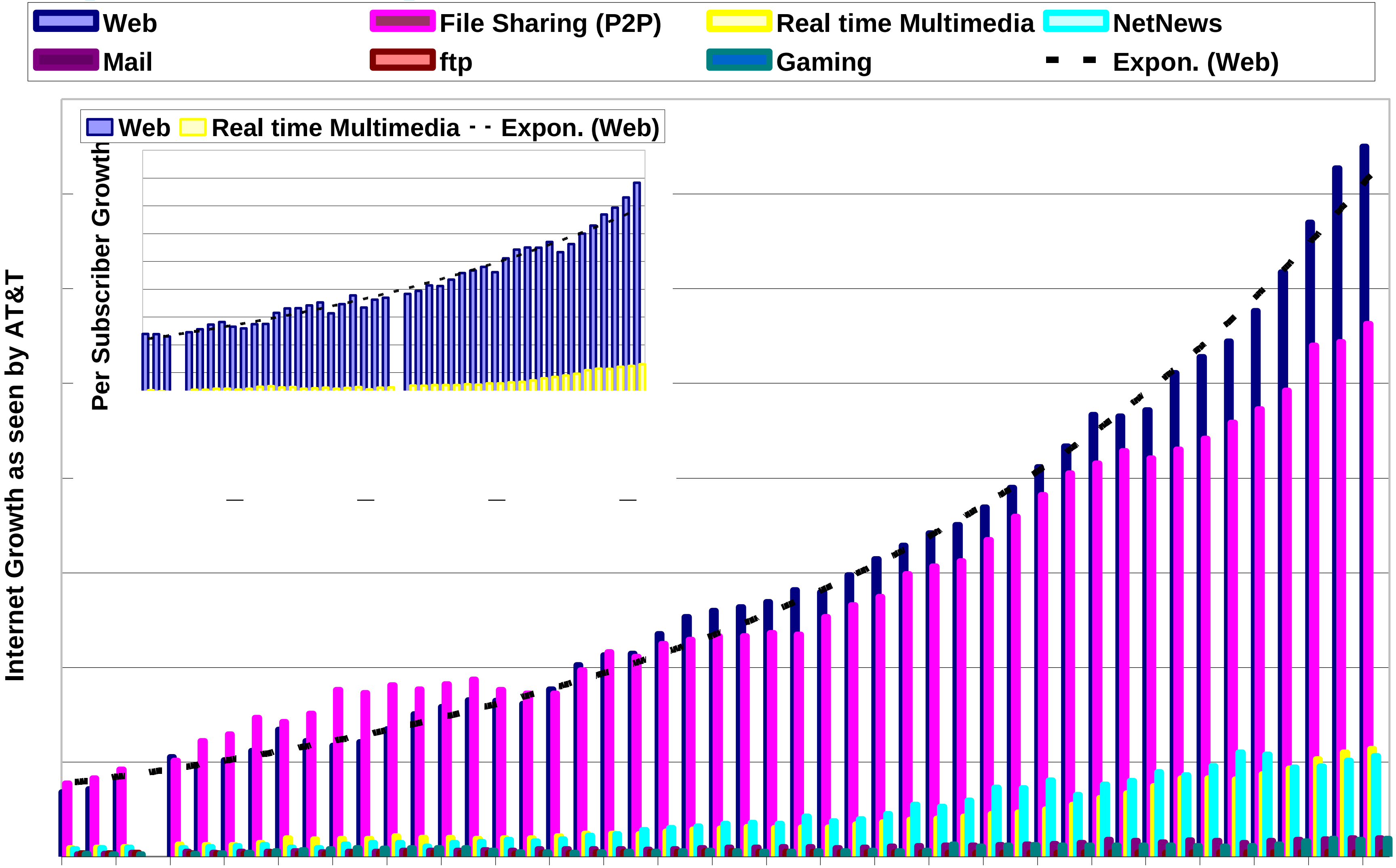
Existing delivered information is estimated to be O(Zettabytes) per year. Most of the new information, and much of the existing is, in any year, on a network – i.e. in flight. Video is responsible for the enormous growth in total amount of information in flight.



Data in Flight includes:

- ***Transactional***
- ***Text/image***
- ***Speech***
- ***Sound (e.g. music)***
- ***Video***

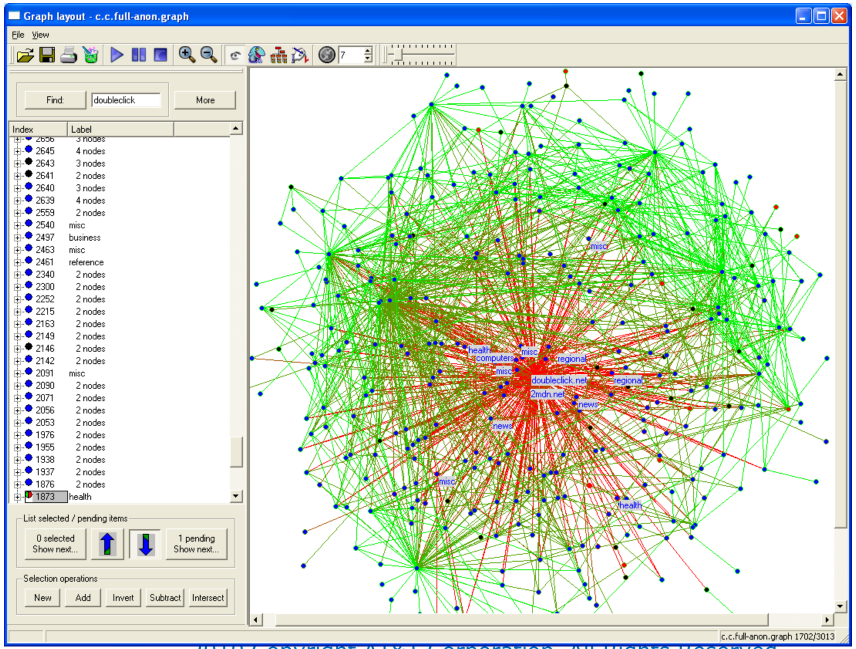
Exponentially More Volume: IP Traffic



Data: Movement, Management, Analysis, Visualization

The scale and power of data related technology continues to increase dramatically. Volume and complexity that would have seemed impossible just a few years ago is now routine. The next bottleneck is Information.

Analysis/Visualization on a Large Graph



Find: doubleclick

Index	Label
2645	4 nodes
2643	3 nodes
2641	2 nodes
2640	3 nodes
2639	4 nodes
2559	2 nodes
2540	misc
2497	business
2463	misc
2461	reference
2340	2 nodes
2300	2 nodes
2252	2 nodes
2215	2 nodes
2163	2 nodes
2149	2 nodes
2146	2 nodes
2142	2 nodes
2091	misc
2090	2 nodes
2071	2 nodes
2056	2 nodes
2053	2 nodes
1976	2 nodes
1955	2 nodes
1938	2 nodes
1937	2 nodes
1876	2 nodes
1873	health

List selected / pending items

0 selected Show next...

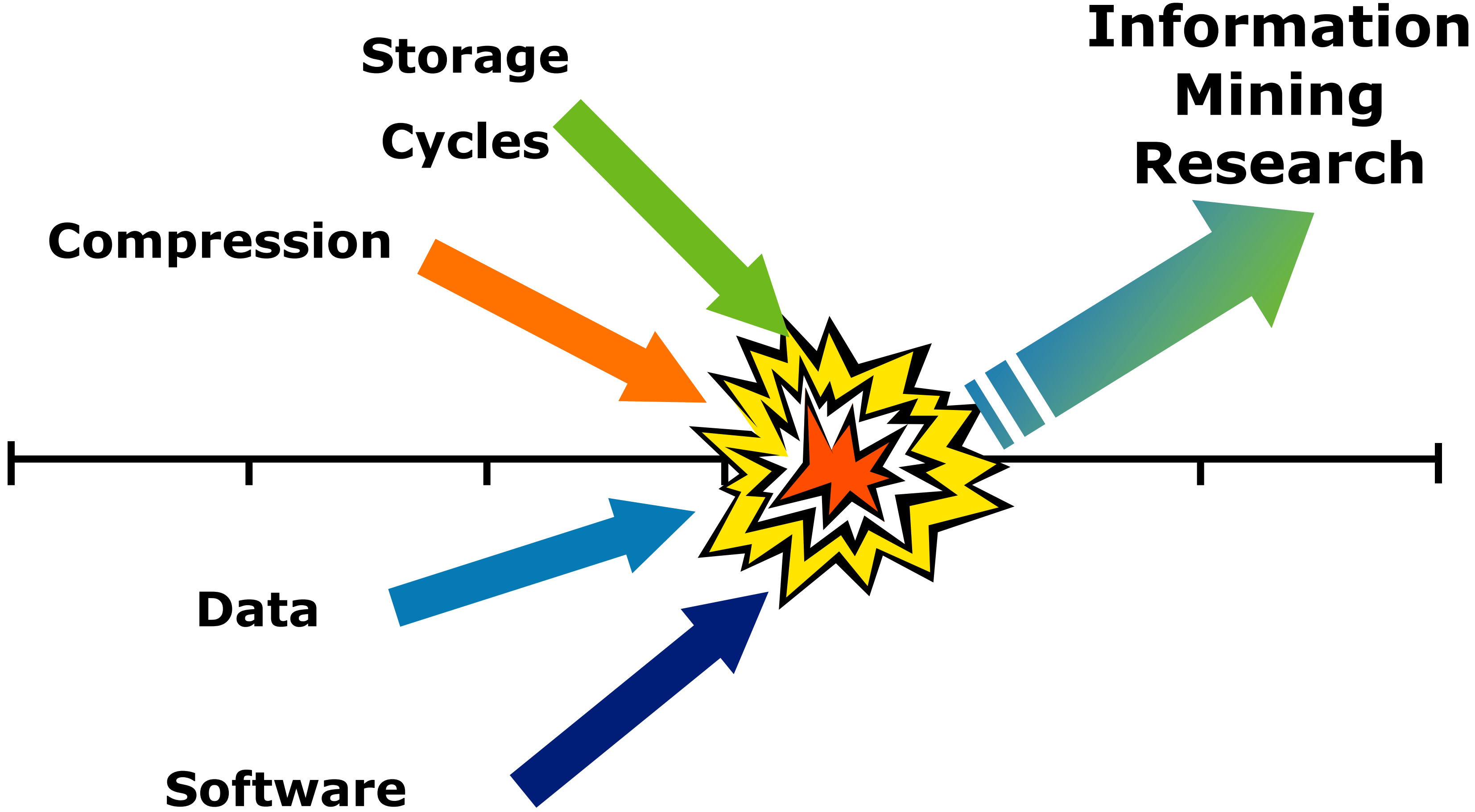
1 pending Show next...

Selection operations

New | Add | Invert | Subtract | Intersect

c.c.full-anon.graph 1702/3013

DRIVING INNOVATION
- Technology Drivers and Trends



Storage

Cycles

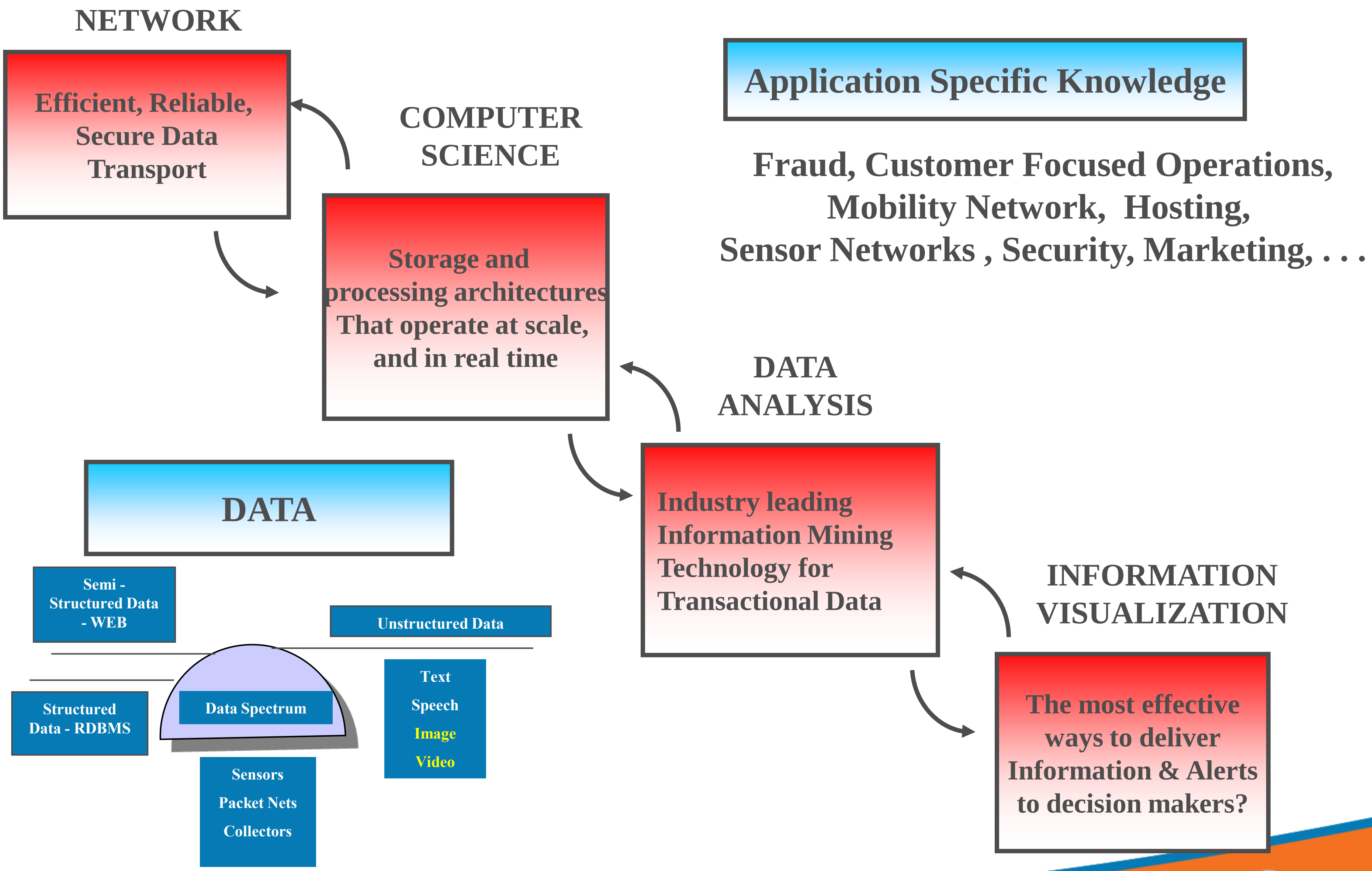
Compression

Data

Software

Information
Mining
Research

AT&T InfoLab



NETWORK

Efficient, Reliable, Secure Data Transport

COMPUTER SCIENCE

Storage and processing architectures That operate at scale, and in real time

DATA ANALYSIS

Industry leading Information Mining Technology for Transactional Data

INFORMATION VISUALIZATION

The most effective ways to deliver Information & Alerts to decision makers?

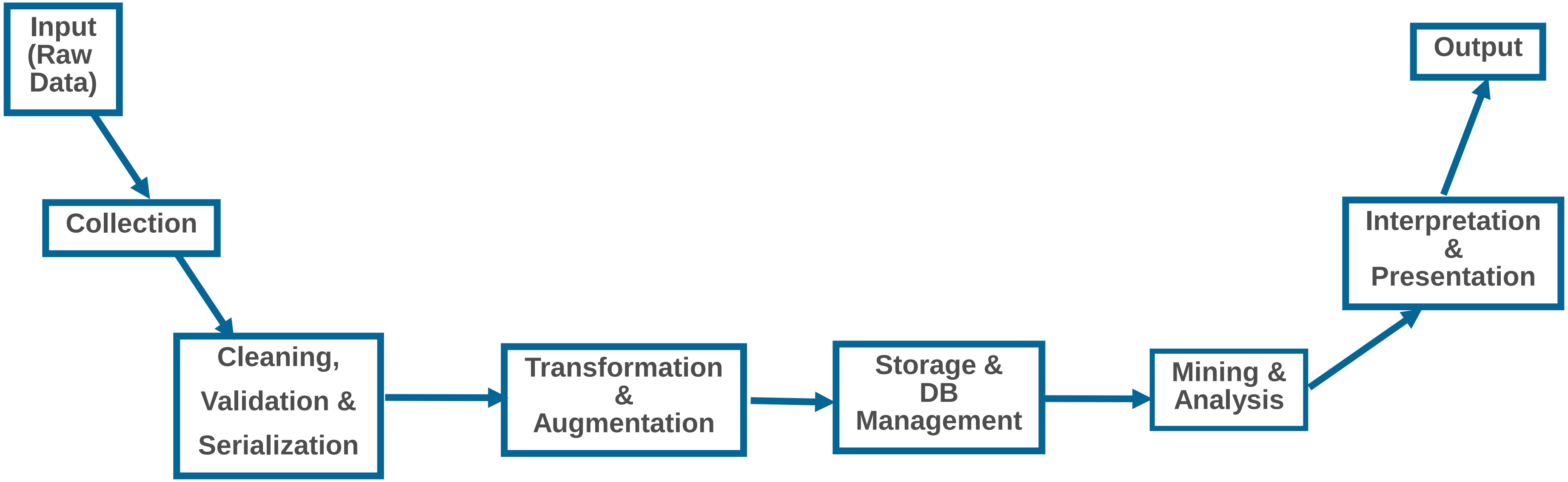
Application Specific Knowledge

Fraud, Customer Focused Operations, Mobility Network, Hosting, Sensor Networks , Security, Marketing, . . .

DATA

Data Lifecycle

Can we completely automate the staging of data for analysis (From origination to analysis ready)?



Input (Raw Data)

Collection

Cleaning, Validation & Serialization

Transformation & Augmentation

Storage & DB Management

Mining & Analysis

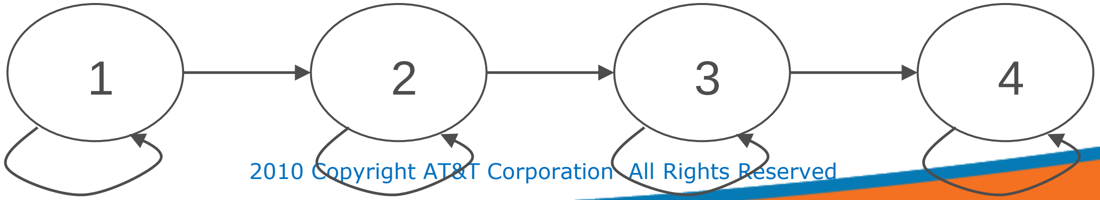
Interpretation & Presentation

Output

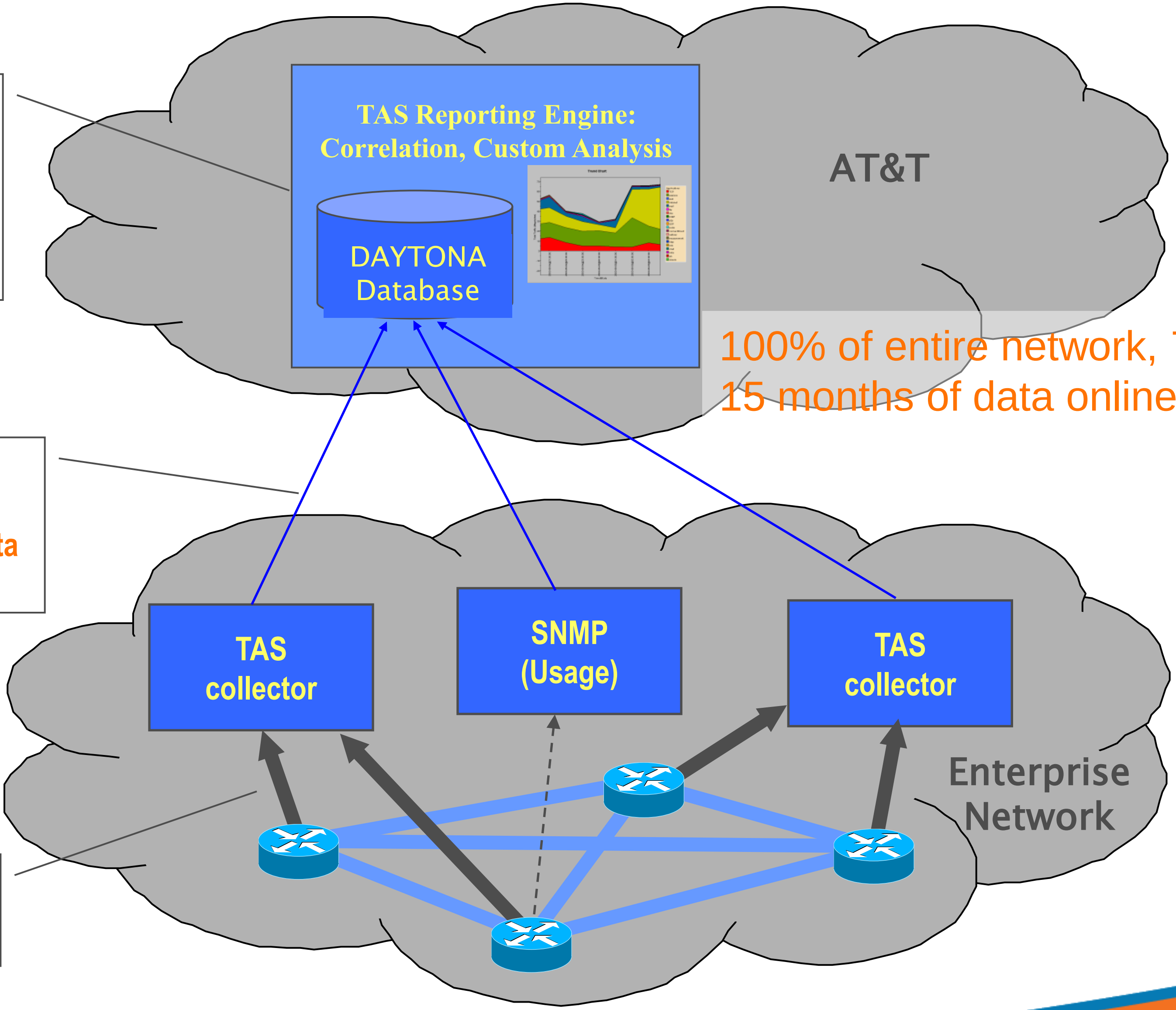
Example: Can the IP Network Run Itself?

- How to push automation as far as possible?
  - Timely, accurate information is essential!!!
  - Tools that separate capabilities from policies, since policies can change fast
    - Example: link utilizations should be < 80% except for links involved in that new VoIP trial in Phoenix with vendor X equipment, where utilizations should be < 50%, except for …
  - Big Guard Rails – extensive monitoring and info correlation/validation
  - Huge Operations involvement at every step
    - Simpler, repeatable tasks/repairs automated

- Smart, transactional network update
  - Deep Just in Time Parse, Semantic Extraction of Router Configurations
  - Integrated with Ticketing, Network Databases, Monitoring, Overarching Policy Control
  - State Transition Paradigm (Policy is Stateful!)



Providing Traffic Analysis for Large IP Networks



Robust storage and presentation tools provide on-demand reporting via web interface

100% of entire network, 7X24, 15 months of data online

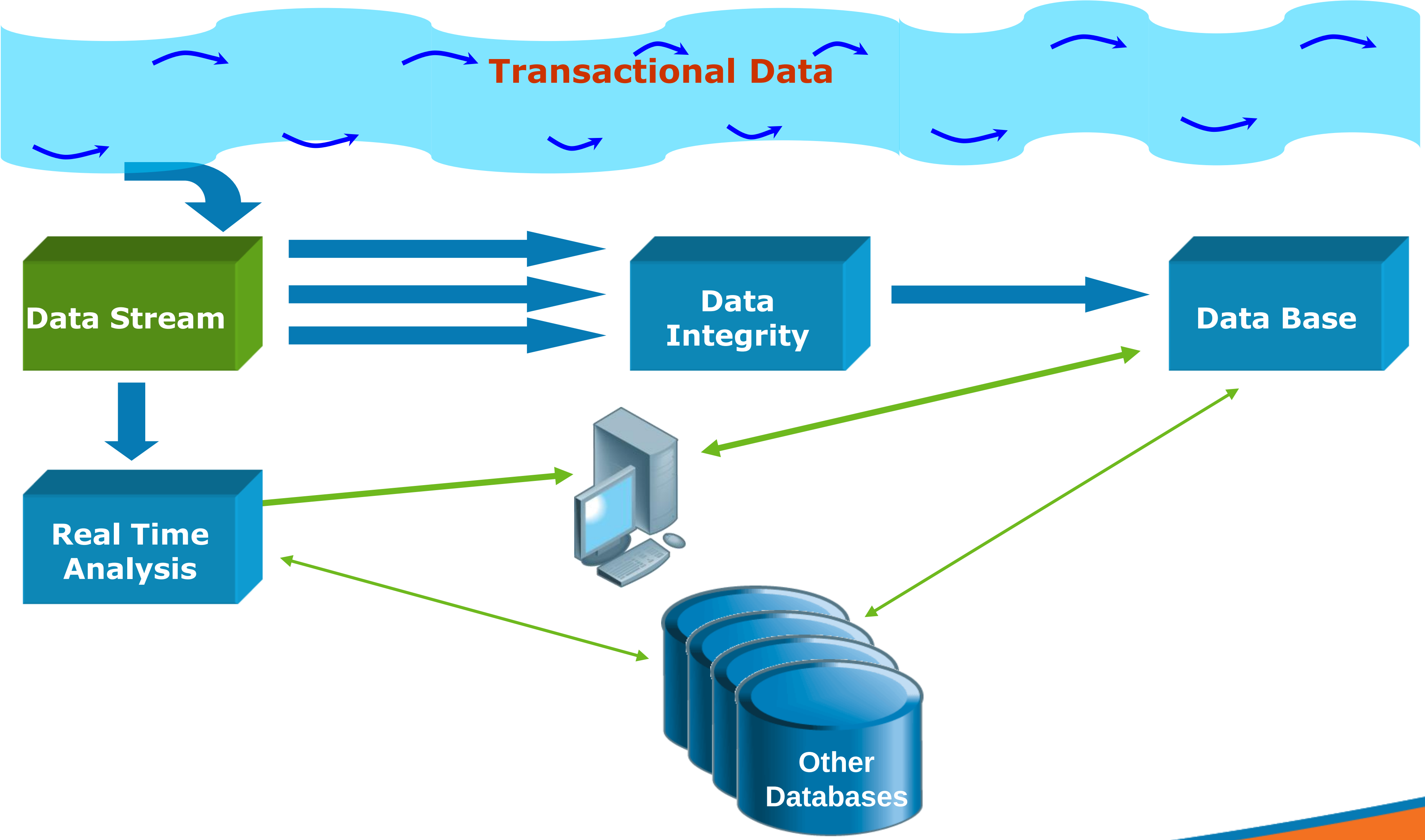
Powerful *Smart Sampling* on TAS collectors reduces data volumes

NetFlow exported from routers

This Takes You From … To …

- From networks consisting of numerous, uncoordinated, error-prone systems
  - e.g., manual grappling with the changing state of the art in packet filters, route maps, IP, MPLS routing, layer 1-3 interworking, …
- To networks where *operators* leverage automated network-wide views to assure performance
  - e.g., “assure negligible customer impact from planned cable intrusion scheduled tonight in New Mexico at midnight, mountain time”
- To networks where *designers* leverage automated mechanisms for real-time network response
  - e.g., “survive any single fiber or router failure with all link utilizations < 70%”
- To networks where VPN *customers* can leverage detailed views of their traffic and flexible, policy-driven routing
  - *e.g., “traffic from east coast customer X sites should prefer X’s Dallas data center and X’s Phoenix Internet Gateway”*

Large Scale Data Management



DSMS + DBMS

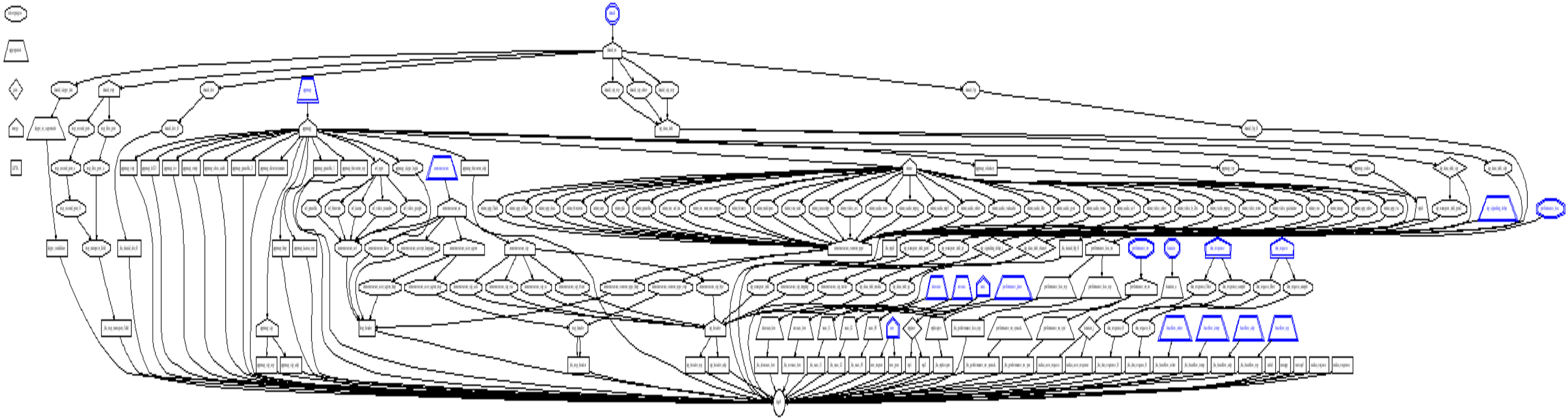
- DBMS – Data *Base* Management System
  - Query data stored on disk.
  - Load via transactions or batch update.
  - Queries can be complex
    - Expensive joins, historical data, etc.
- DSMS – Data *Stream* Management System
  - Analyze records “in flight” – *very* cheap data ingest.
  - Relatively simple queries
    - Must execute in real time.
    - Limited historical analysis.

Network Monitoring via GSQL

- Simple

```
Select tb, SrcIP, DestIP, count(*)
From TCP
Group By tb, SrcIP, DestIP
```

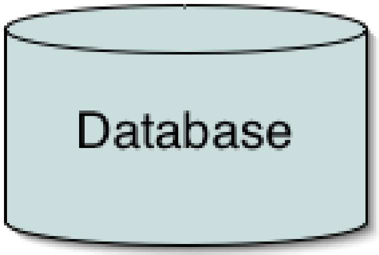
- Flexible
  - Auto-configuration to monitor selected network interfaces.
    - Complex queries via composition.
- Optimizable



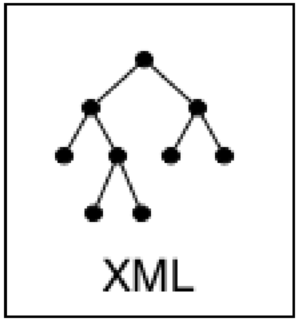
Data, data, everywhere!

Incredible amounts of data are stored in well-behaved formats:

Databases:



XML:

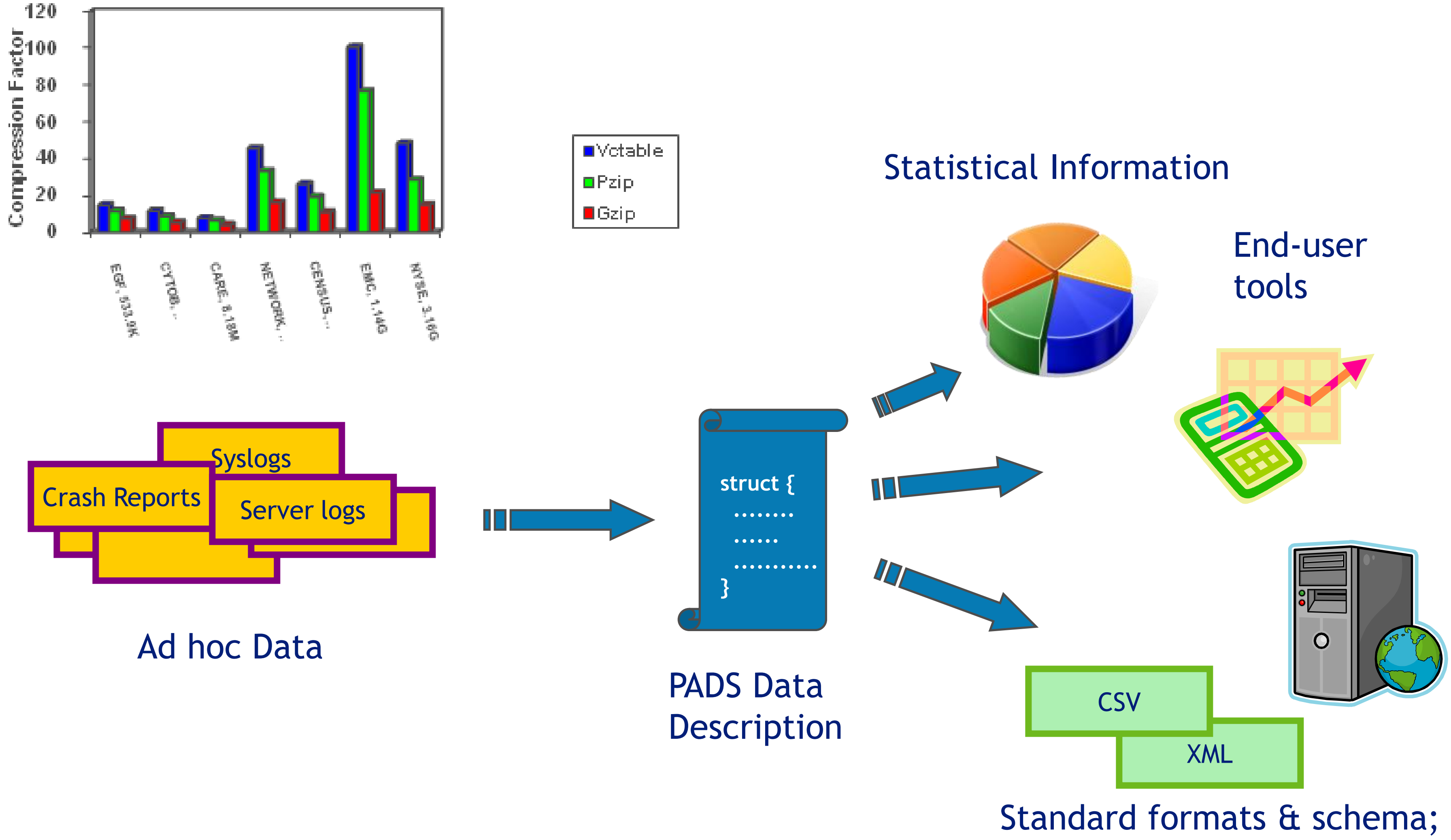


Vast amounts of chaotic *ad hoc* data from logs, legacy systems, *etc*. exist as well.

Lots of data are not in well-behaved formats with ready tool support.

Data Transformation:

Compression – Redundancy – Encryption - Reformating



Statistical Information

End-user tools

Ad hoc Data

PADS Data Description

Standard formats & schema;

Examples of Ad Hoc Data

It is difficult to define a*d hoc data* precisely: it is less formalized than data in relational databases or xml, but more structured than free-form text.   To give a feel for the variety, we give some examples.

Binary data: DNS packets

```
00000000: 9192 d8fb 8480 0001 05d8 0000 0000 0872  ...............r
00000010: 6573 6561 7263 6803 6174 7403 636f 6d00  esearch.att.com.
00000020: 00fc 0001 c00c 0006 0001 0000 0e10 0027  ...............'
00000030: 036e 7331 c00c 0a68 6f73 746d 6173 7465  .ns1...hostmaste
00000040: 72c0 0c77 64e5 4900 000e 1000 0003 8400  r..wd.I.........
```

ASCII data: Option price trading authority

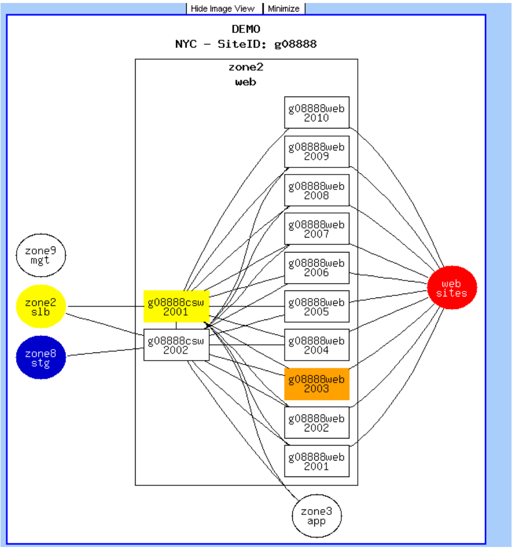
```
HL00000002START OF OPEN INTEREST
d 00000003FZYX G1AB0000030000300000
HM00000004END OF OPEN INTEREST
HE00000005START OF SUMMARY
f 00000006NYZX B1QB00052000120000070000B000050000000520000
  00490000005100+00000100B00000005300000052500000535000
HF00000007END OF SUMMARY
k 00000008LYXW B1KB0000065G0000009900100000001000020000
```

Binary and ASCII are both important forms of ad hoc data.

Decide – Analysis & Visualization

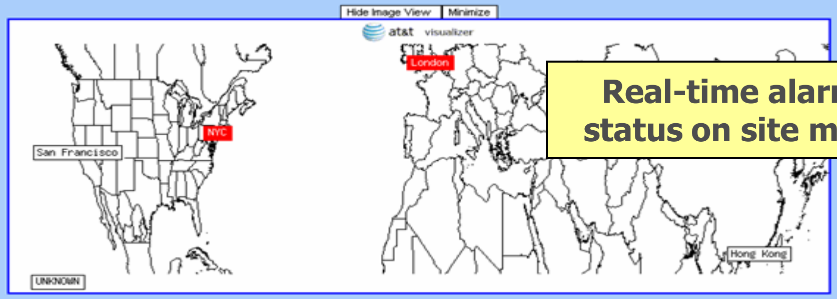
The amount and variety of data are far too great for all but the most powerful tools. Robust, automated analysis is essential to control in real time. Humans are still the best visual pattern recognition engines available.

An example of a small system

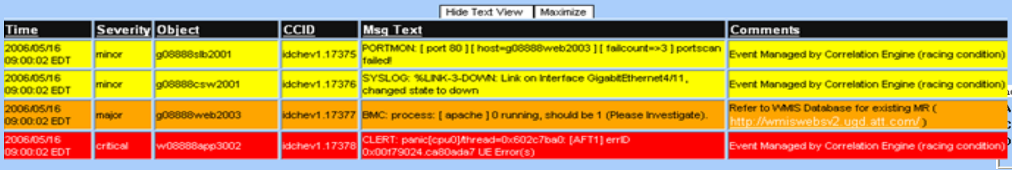


Visualizer

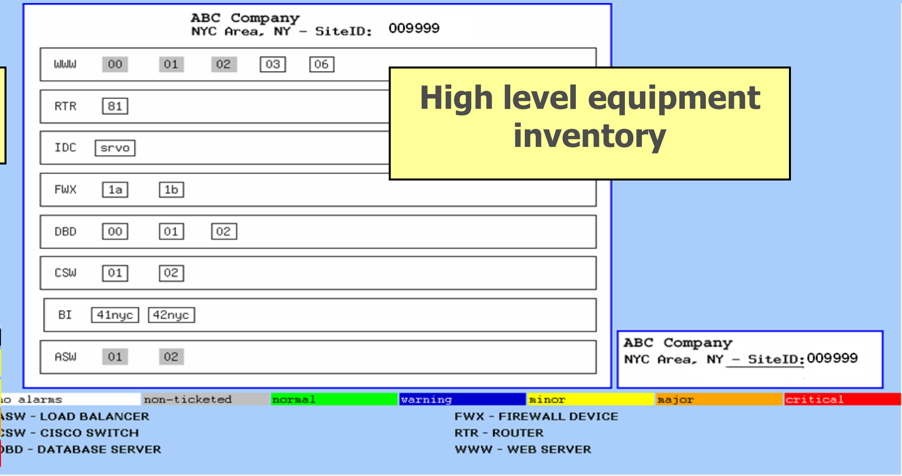
Managing Systems Distributed Worldwide



Real-time alarm status on site map



Time	Severity	Object	CCID	Msg Text	Comments
2006/05/16 09:00:02 EDT	minor	g08888slb2001	idchev1.17375	PORTMON: [port 80] [host=g08888web2003] [failcount=>3] portscan failed!	Event Managed by Correlation Engine (racing condition)
2006/05/16 09:00:02 EDT	minor	g08888csw2001	idchev1.17376	SYSLOG: %LINK-3-DOWN: Link on Interface GigabitEthernet4/11, changed state to down	Event Managed by Correlation Engine (racing condition)
2006/05/16 09:00:02 EDT	major	g08888web2003	idchev1.17377	BMC: process: [apache] 0 running, should be 1 (Please Investigate).	Refer to WMIS Database for existing MR (http://wmiswebsv2.ugd.att.com/)
2006/05/16 09:00:02 EDT	critical	w08888app3002	idchev1.17378	CLERT: panic[cpu0]/thread=0x602c7ba0: [AFT1] errID 0x00f79024.ca80ada7 UE Error(s)	Event Managed by Correlation Engine (racing condition)



ABC Company
NYC Area, NY – SiteID: 009999

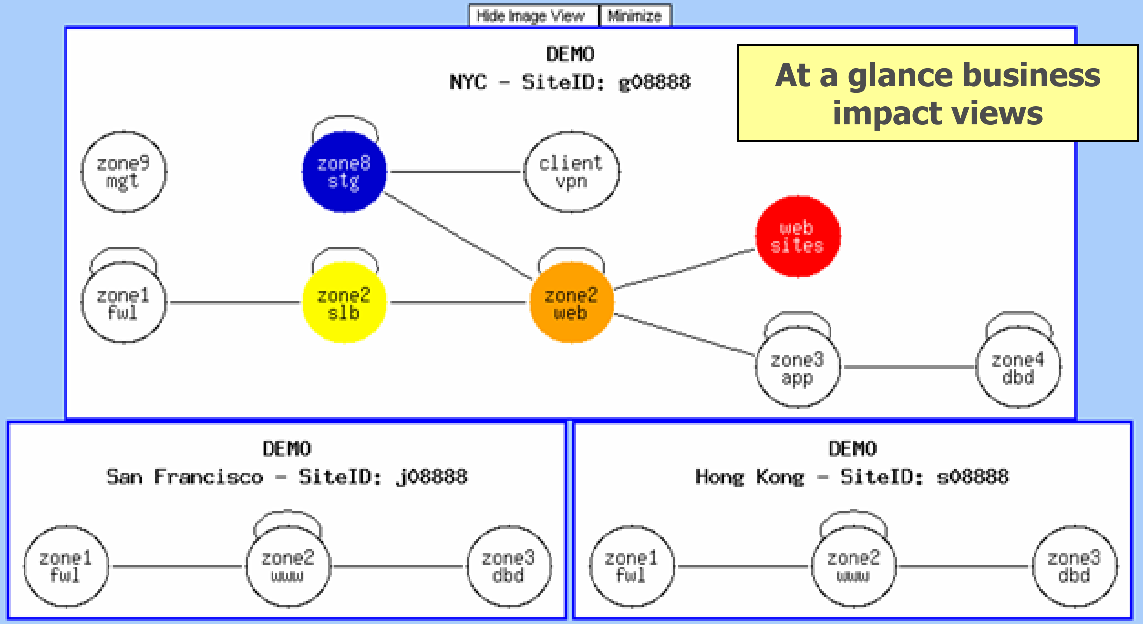
WWW 00 01 02 03 06
RTR 81
IDC srvo
FWX 1a 1b
DBD 00 01 02
CSW 01 02
BI 41nyc 42nyc
ASW 01 02

ABC Company
NYC Area, NY – SiteID:009999

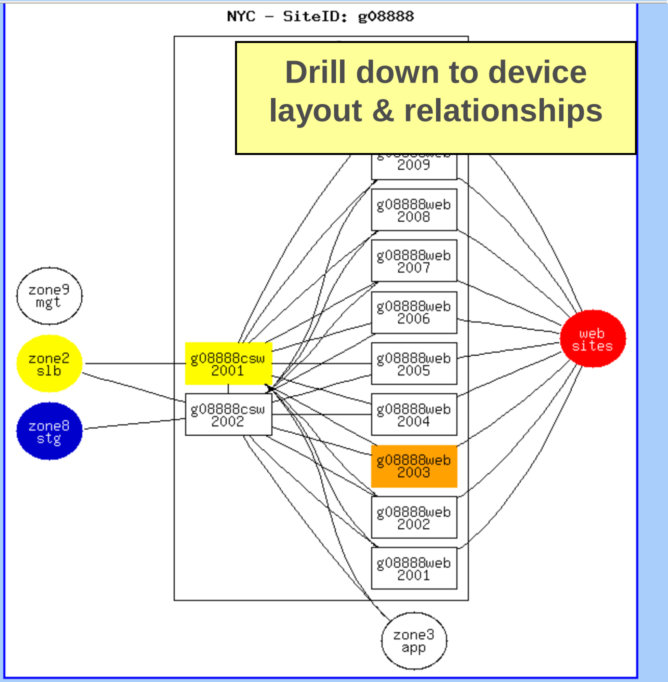
no alarms | non-ticketed | normal | warning | minor | major | critical

ASW - LOAD BALANCER
CSW - CISCO SWITCH
DBD - DATABASE SERVER
FWX - FIREWALL DEVICE
RTR - ROUTER
WWW - WEB SERVER

High level equipment inventory



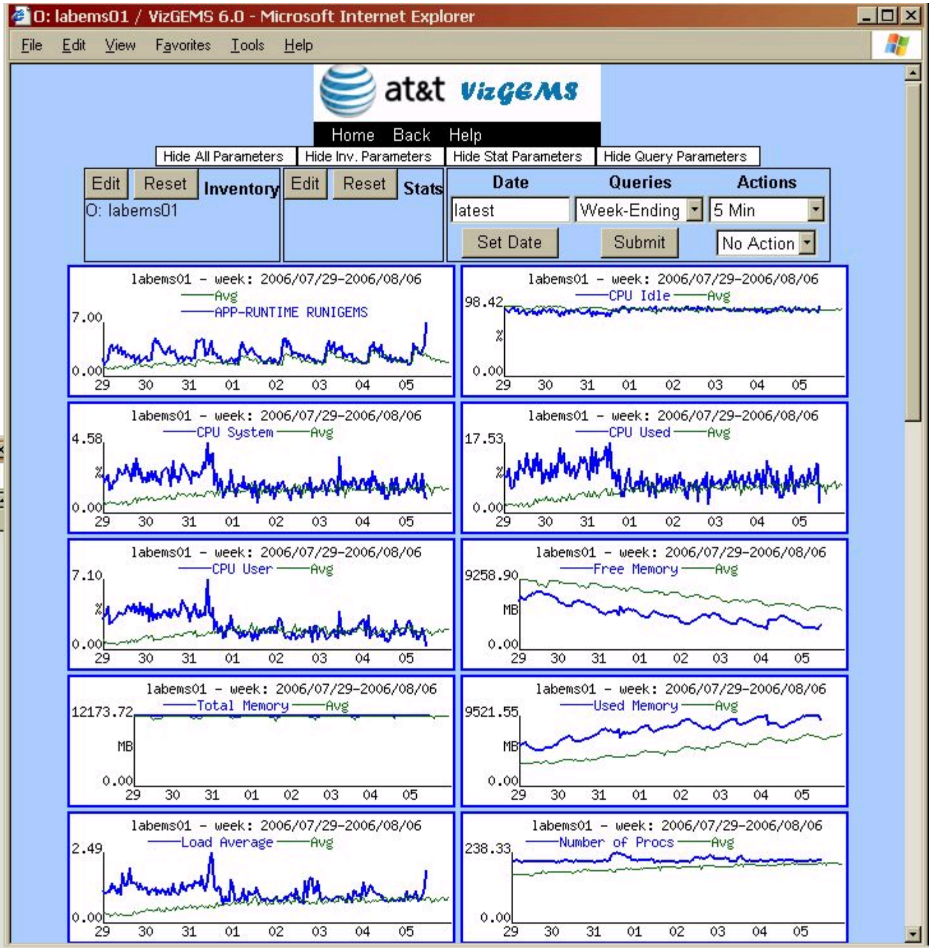
At a glance business impact views



Drill down to device layout & relationships

Enhanced Control of Networks and Servers

- Early identification of trends
- Control charts identify unusual conditions
- Dramatic reduction of unnecessary alarms
- Complete drill down for fast resolution of problems
- Visual query capability
- All views, e.g. physical/logical, related



O: labems01 / VizGEMS 6.0 - Microsoft Internet Explorer

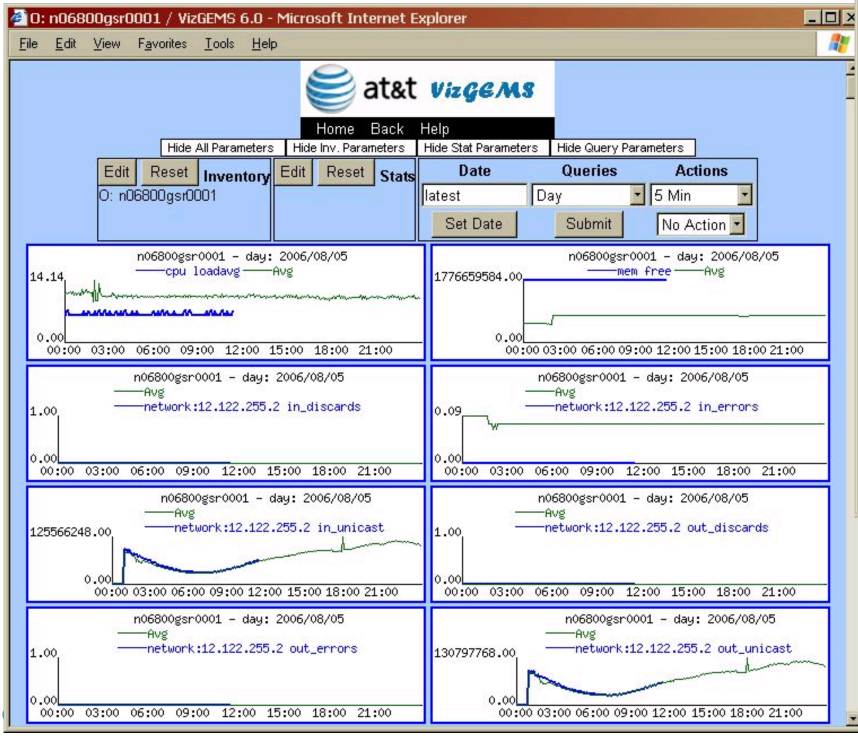
Inventory: O: labems01

Date: latest

Queries: Week-Ending

Actions: 5 Min

No Action



O: n06800gsr0001 / VizGEMS 6.0 - Microsoft Internet Explorer

Inventory: O: n06800gsr0001

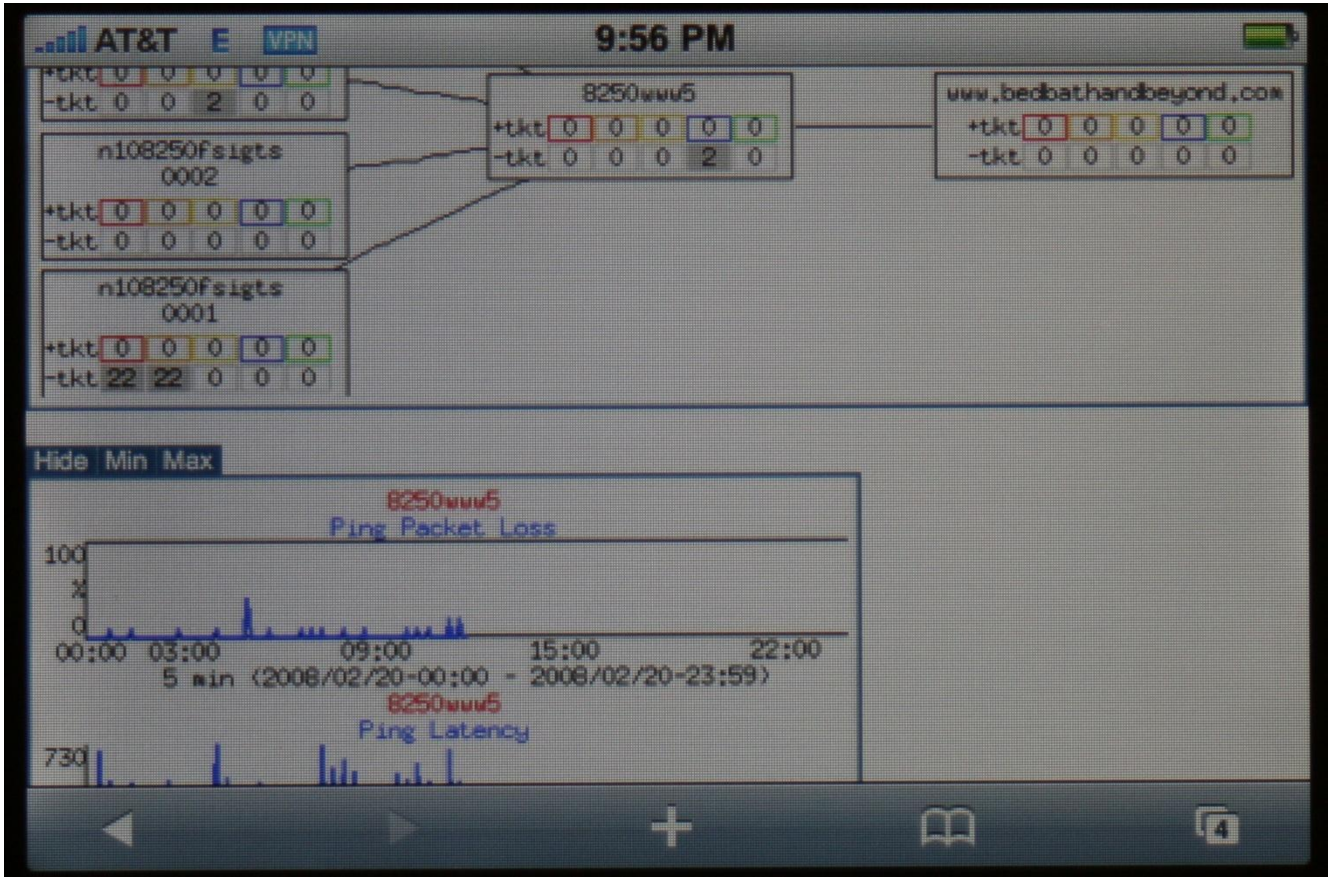
Date: latest

Queries: Day

Actions: 5 Min

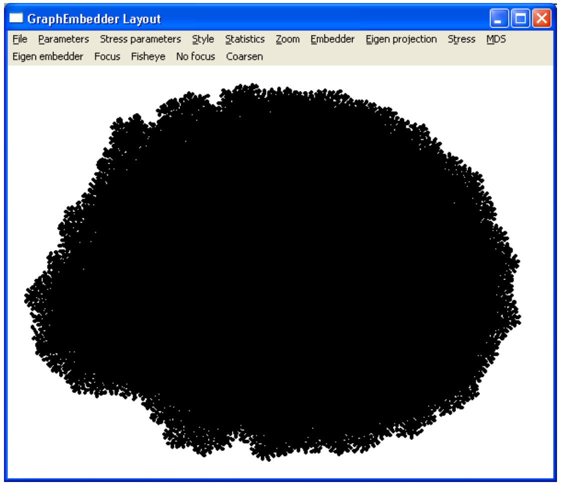
No Action

Transparency - Anywhere, Anytime



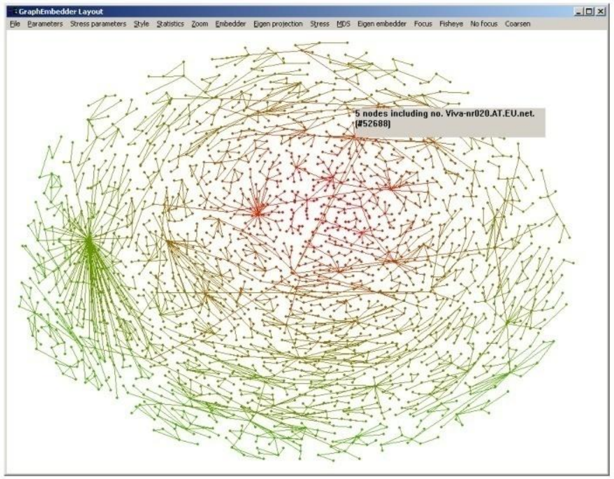
Topview: exploring large networks by topological zooming

- Large networks are everywhere.


GraphEmbedder Layout
File Parameters Stress parameters Style Statistics Zoom Embedder Eigen projection Stress MDS
Eigen embedder Focus Fisheye No focus Coarsen

- Visualization problem: complexity, clutter, occlusion, visual overload

- Topview: interactive adjustable focus
  - high level of detail near a focus
  - progressively less detail further away
  the view always reflects the original structure “semantic zooming”


GraphEmbedder Layout
File Parameters Stress parameters Style Statistics Zoom Embedder Eigen projection Stress MDS Eigen embedder Focus Fisheye No focus Coarsen

5 nodes including no. Viva-nr020.AT.EU.net.
(#52688)

data courtesy Bill Cheswick, Lumeta Corp.

Talkalytics

Speech analytics system for optimizing operational efficiencies and improving customer satisfaction; currently in beta supporting nearly 100 analysts

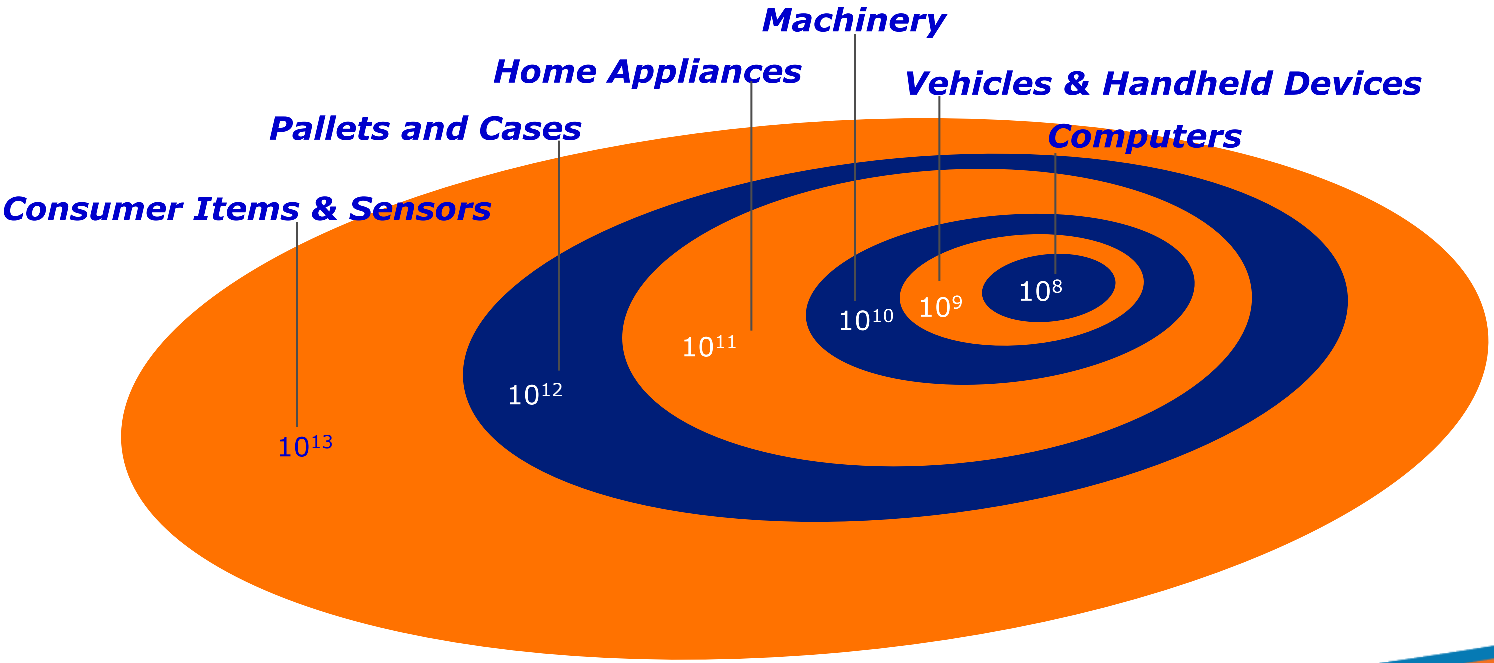
Audio Search: Based on AT&T's WATSON technologies; *Over one billion* words processed this year.

Customer Experience: Integrates customer experience surveys with call records to enable instant global and collaborative search among analysts

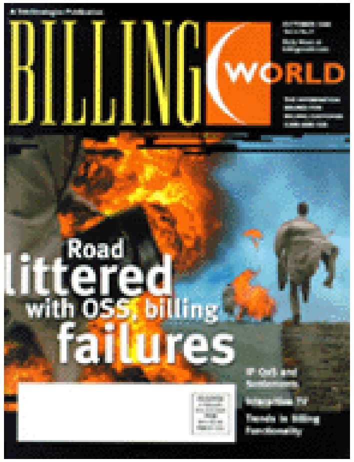
Analytics: Supports for trend analysis and summary reports by call reason, regions, agent, customer satisfaction metrics, etc.

Conclusions

Advances in operations over the past decade have been in orders of magnitude, driven by needs of applications such as: IP, Mobility, Web, and Sensors, and improvements in systems and analytic technologies.



- Nature of Analytics Changes
- Optimize Speed vs. Accuracy Tradeoffs
- Depth & Volatility: Rules vs. Differences
- Data Management of near real time, Interactive, and Record & Playback Visualization
- Real Time Data Quality Assessment & Improvement



- Source of Fundamental Automation & Organizational Change
- Heterogeneous Event Stream Management & Query
- Database Integration, Approximate Matching
- Data Management for Interactive Visualization
- Data Feed Management
- Real time data quality

Selected Research Directions

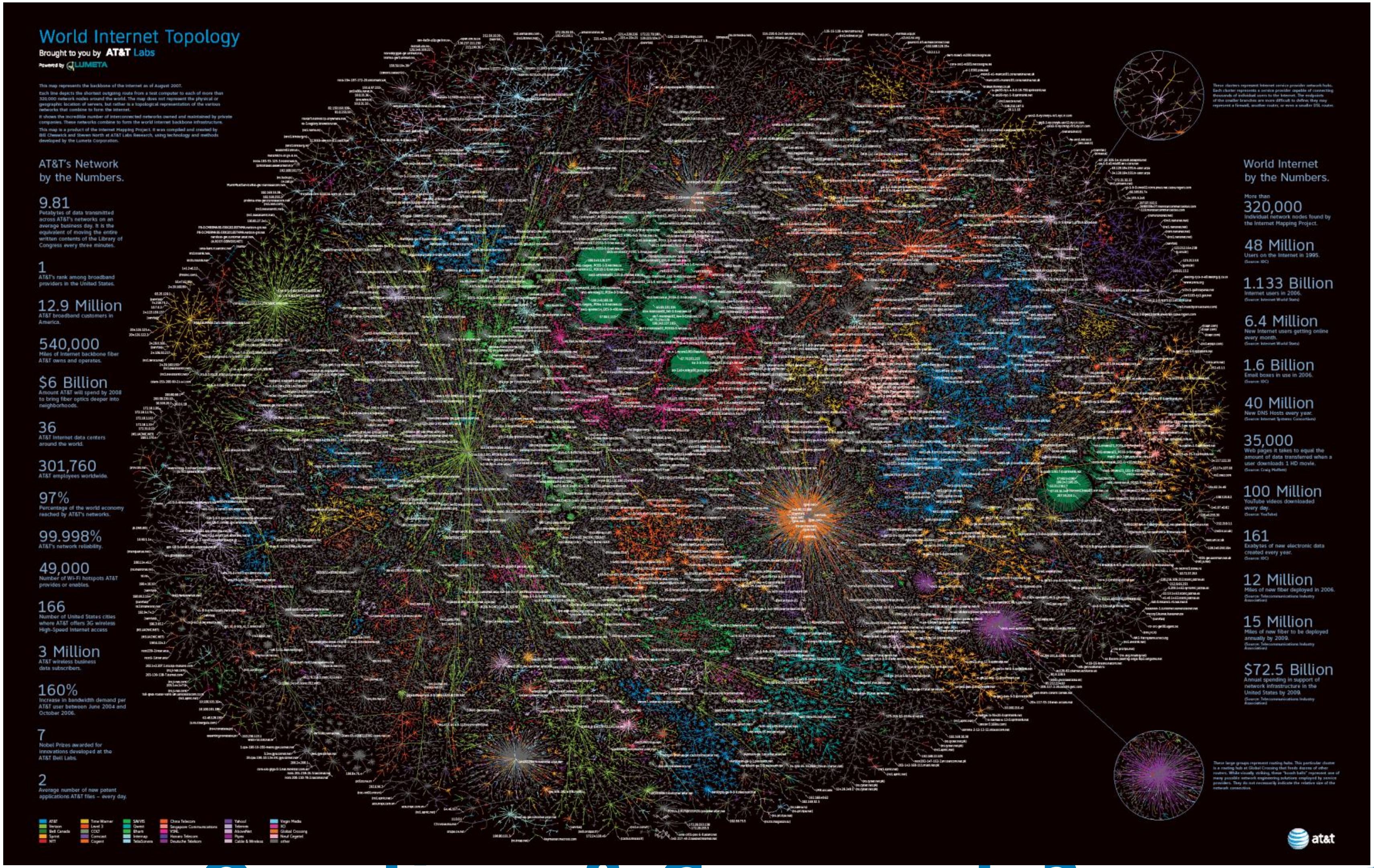
The Next 5 Years

Pervasive:

- Scale
- Security
- Mobility
- Operations
- Reliability

- **Network Based Computing:** **Corporate grade "cloud" computing will be routinely employed in critical applications. Location and Presence.**
- **Rich Media:** **Mission critical, interactive applications will employ multimedia and move seamlessly between all 3 canonical screens.**
- **Networks (including Internet) of everything:** **Billions of devices, many mobile, will interact as computing, sensing, and communications platforms.**
- **Information Leverage:** **Collection, Analysis, Visualization, & Distribution will include all forms of data (e.g. Relational, Semi-Structured, Text, Speech, Video, Image) integrated, near real time, and at huge scale.**
- **Communities of Interest:** **Collaboration, Social Networks, Group Oriented Services.**

Thank You!



World Internet Topology

Brought to you by **AT&T** Labs

Powered by LUMETA

This map represents the backbone of the Internet as of August 2007.

Each line depicts the shortest outgoing route from a test computer to each of more than 320,000 network nodes around the world. The map does not represent the physical or geographic location of servers, but rather is a topological representation of the various networks that combine to form the Internet.

It shows the incredible number of interconnected networks owned and maintained by private companies. These networks combine to form the world Internet backbone infrastructure.

This map is a product of the Internet Mapping Project. It was compiled and created by Bill Cheswick and Steven North at AT&T Labs Research, using technology and methods developed by the Lumeta Corporation.

AT&T's Network by the Numbers.

9.81
Petabytes of data transmitted across AT&T's networks on an average business day. It is the equivalent of moving the entire written contents of the Library of Congress every three minutes.

1
AT&T's rank among broadband providers in the United States.

12.9 Million
AT&T broadband customers in America.

540,000
Miles of Internet backbone fiber AT&T owns and operates.

$6 Billion
Amount AT&T will spend by 2008 to bring fiber optics deeper into neighborhoods.

36
AT&T Internet data centers around the world.

301,760
AT&T employees worldwide.

97%
Percentage of the world economy reached by AT&T's networks.

99.998%
AT&T's network reliability.

49,000
Number of Wi-Fi hotspots AT&T provides or enables.

166
Number of United States cities where AT&T offers 3G wireless High-Speed Internet access

3 Million
AT&T wireless business data subscribers.

160%
Increase in bandwidth demand per AT&T user between June 2004 and October 2006.

7
Nobel Prizes awarded for innovations developed at the AT&T Bell Labs.

2
Average number of new patent applications AT&T files – every day.

These clusters represent Internet service provider network hubs. Each cluster represents a service provider capable of connecting thousands of individual users to the Internet. The endpoints of the smaller branches are more difficult to define; they may represent a firewall, another router, or even a smaller DSL router.

World Internet by the Numbers.

More than
320,000
Individual network nodes found by the Internet Mapping Project.

48 Million
Users on the Internet in 1995.
(Source: IDC)

1.133 Billion
Internet users in 2006.
(Source: Internet World Stats)

6.4 Million
New Internet users getting online every month.
(Source: Internet World Stats)

1.6 Billion
Email boxes in use in 2006.
(Source: IDC)

40 Million
New DNS Hosts every year.
(Source: Internet Systems Consortium)

35,000
Web pages it takes to equal the amount of data transferred when a user downloads 1 HD movie.
(Source: Craig Moffett)

100 Million
YouTube videos downloaded every day.
(Source: YouTube)

161
Exabytes of new electronic data created every year.
(Source: IDC)

12 Million
Miles of new fiber deployed in 2006.
(Source: Telecommunications Industry Association)

15 Million
Miles of new fiber to be deployed annually by 2009.
(Source: Telecommunications Industry Association)

$72.5 Billion
Annual spending in support of network infrastructure in the United States by 2009.
(Source: Telecommunications Industry Association)

These large groups represent routing hubs. This particular cluster is a routing hub at Global Crossing that feeds dozens of other routers. While visually striking, these "bush balls" represent one of many possible network engineering solutions employed by service providers. They do not necessarily indicate the relative size of the network connection.

Questions & Comments?